

Method for access protection

Patent number: DE3512785
Publication date: 1986-10-23
Inventor: METZENDORF HEINRICH DR RER NAT (DE)
Applicant: TELEFONBAU & NORMALZEIT GMBH (DE)
Classification:
- **International:** G06F3/08; G07F7/10; G06K7/00; G06K19/00;
G11C17/00; B44F1/12; H04L11/26
- **European:** G07C9/00C2B; G06F1/00N5A2; G06F21/00N5A2
Application number: DE19853512785 19850410
Priority number(s): DE19853512785 19850410

Abstract of DE3512785

The use of a terminal of a data processing facility or data processing system or telecommunication switching system is enabled by the user in-putting a key number or a password via the input keyboard, a storage device with an interchangeable small and handy data carrier, connected to the terminal, containing the key number or the password at a particular storage location and the terminal being enabled in the case of a correspondence with the key number or the password input.

Data supplied from the esp@cenet database - Worldwide

⑩ BUNDESREPUBLIK
DEUTSCHLAND



DEUTSCHES
PATENTAMT

⑪ Offenlegungsschrift
DE 35 12 785 A 1

⑫ Aktenzeichen: P 35 12 785.6
⑬ Anmeldetag: 10. 4. 85
⑭ Offenlegungstag: 23. 10. 86

⑮ Int. Cl. 4:
G 06 F 3/08

G 07 F 7/10
G 08 K 7/00
G 08 K 19/00
G 11 C 17/00
B 44 F 1/12
H 04 L 11/28

DE 35 12 785 A 1

⑰ Anmelder:

Telefonbau und Normalzeit GmbH, 6000 Frankfurt,
DE

⑱ Erfinder:

Metzendorf, Heinrich, Dr.rer.nat., 6082 Mörfelden,
DE

⑲ Verfahren zur Zugriffssicherung

Die Benutzung eines Endgeräts einer Datenverarbeitungseinrichtung oder Datenverarbeitungsanlage oder Fernmeldevermittlungsanlage wird dadurch freigegeben, daß der Benutzer eine Schlüsselzahl oder ein Paßwort über die Eingabetastatur eingibt, wobei eine am Endgerät angeschlossene Speichereinrichtung mit einem auswechselbaren, kleinen und handlichen Datenträger auf einem bestimmten Speicherplatz die Schlüsselzahl oder das Paßwort enthält und bei Übereinstimmung mit der eingegebenen Schlüsselzahl oder dem Paßwort eine Freigabe des Endgeräts erfolgt.

DE 35 12 785 A 1

3512785

Telefonbau und Normalzeit GmbH, Postfach 4432, 6000 Frankfurt/M.

Verfahren zur Zugriffssicherung

P a t e n t a n s p r ü c h e :

1. Verfahren zur Zugriffssicherung für ein mit einer Speichereinrichtung mit auswechselbaren Datenträgern verbundenes, eine Eingabetastatur aufweisendes Endgerät einer Datenverarbeitungseinrichtung, beispielsweise Personalcomputer, einer Datenverarbeitungs- oder Fernmeldevermittlungsanlage durch Eingabe einer Schlüsselzahl oder eines Paßwortes, welches mit einer eingespeicherten Schlüsselzahl oder Paßwort verglichen wird und nur bei Übereinstimmung eine Benutzung des Endgeräts bzw. der Datenverarbeitungsanlage oder der Fernmeldevermittlungsanlage möglich ist, dadurch gekennzeichnet,
daß bei Inbetriebnahme des Endgeräts von einem Adressgenerator eine Adresse bereitgestellt wird, daß mit dieser Adresse ein Speicherplatz des Datenträgers angesteuert und die dort eingespeicherte Schlüsselzahl oder das Paßwort ausgelesen wird und daß anschließend der Benutzer beispielsweise über eine Anzeigevorrichtung des Endgeräts zur Eingabe der Schlüsselzahl oder des Paßworts aufgefordert wird, wobei der betreffende Speicherplatz für die Einspeicherung anderer Daten gesperrt ist.

3512785

2. Verfahren nach Anspruch 1,
dadurch gekennzeichnet,
daß die Speichereinrichtung einen kleinen, handlichen
Datenträger, beispielsweise Mikro Floppy Disk, Mikro-
kassette, usw., aufweist.
3. Verfahren nach Anspruch 1 oder 2,
dadurch gekennzeichnet,
daß nach Einlegen des Datenträgers in die Speicherein-
richtung selbsttätig der die Schlüsselzahl oder Paßwort
enthaltene Speicherplatz des Datenträgers ausgelesen wird.
4. Verfahren nach Anspruch 1 oder 2,
dadurch gekennzeichnet,
daß bei eingelegtem Datenträger nach Betätigung einer be-
stimmten Taste der Eingabetastatur selbsttätig der die
Schlüsselzahl oder Paßwort enthaltene Speicherplatz des
Datenträgers ausgelesen wird.
5. Verfahren nach einem der Ansprüche 1 bis 4,
dadurch gekennzeichnet,
daß nach Herausnehmen des Datenträgers aus der Speicherein-
richtung bzw. nach Betätigung einer bestimmten Taste die
Benutzung des Endgeräts, der Datenverarbeitungsanlage oder
der Fernmeldevermittlungsanlage gesperrt wird.
6. Verfahren nach einem der Ansprüche 1 bis 4,
dadurch gekennzeichnet,
daß nach Ablauf einer vorgegebenen Zeit, in der keine
Benutzung des Endgeräts, der Datenverarbeitungsanlage oder
der Fernmeldevermittlungsanlage stattgefunden hat, die Be-
nutzung gesperrt wird.

7. Verfahren nach einem der Ansprüche 1 bis 5,
dadurch gekennzeichnet,
daß nach Freigabe der Benutzung eine andere Schlüsselzahl
oder Paßwort in den Speicherplatz des Datenträgers ein-
tragbar ist.
8. Verfahren nach einem der Ansprüche 1 bis 6,
dadurch gekennzeichnet,
daß die Adresse des Speicherplatzes über die Eingabetastatur
veränderbar ist.
9. Verfahren nach einem der Ansprüche 1 bis 6,
dadurch gekennzeichnet,
daß der Adressgenerator selbsttätig die Adresse verändert.
10. Verfahren nach einem der Ansprüche 1 bis 9,
dadurch gekennzeichnet,
daß die Benutzungssperre auf bestimmte Anwendungsarten
oder Prozeduren beschränkt ist.

P 3954

25.3.1985

Fs/Mc.

Verfahren zur Zugriffssicherung

Die Erfindung betrifft ein Verfahren zur Zugriffssicherung für ein mit einer Speichereinrichtung mit auswechselbaren Datenträgern verbundenes, eine Eingabetastatur aufweisendes Endgerät einer Datenverarbeitungseinrichtung, beispielsweise Personalcomputer, einer Datenverarbeitungs- oder Fernmeldevermittlungsanlage durch Eingabe einer Schlüsselzahl oder eines Paßwortes, welches mit einer eingespeicherten Schlüsselzahl oder Paßwort verglichen wird und nur bei Übereinstimmung eine Benutzung des Endgeräts bzw. der Datenverarbeitungsanlage oder Fernmeldevermittlungsanlage möglich ist.

Die Verwendung einer Schlüsselzahl zur autorisierten Benutzung von Diensten oder Geräten in der Fernmeldetechnik ist bereits bekannt (s. Oden, Nachrichtenvermittlung, Oldenbourg Verlag, München, Wien, 1975, Seite 54). Durch Eingabe der nur ihm bekannten Schlüsselzahl weist sich der Benutzer gegenüber dem Endgerät bzw. der Anlage als autorisiert aus.

Eine noch größere Sicherheit gegen unbefugte Benutzung bietet eine sogenannte Chipkarte, mit der sich der Benutzer dem Endgerät oder der Anlage gegenüber als autorisiert ausweist. Diese Chipkarte enthält entsprechende Informationen, die von einem Chipkartenleser gelesen werden, wobei die Weiterbehandlung der eingespeicherten Informationen wie bei der Schlüsselzahl oder dem Paßwort erfolgt. Die Verwendung einer Chipkarte setzt jedoch einen entsprechenden Chipkartenleser voraus, welcher beispielsweise Bestandteil des Endgeräts sein kann. Derartige Endgeräte sind beispielsweise in der Druckschrift

"telcomreport" 8 (1985) Heft 1, auf Seite 14, beschrieben.

Die Aufgabe der Erfindung besteht nun darin, ein Verfahren anzugeben, welches die gleiche Sicherheit wie eine Chipkarte bietet, ohne daß hierbei zusätzlich aufwendige Lesevorrichtungen benötigt werden.

Diese Aufgabe wird dadurch gelöst, daß bei Inbetriebnahme des Endgeräts von einem Adressgenerator eine Adresse bereitgestellt wird, daß mit dieser Adresse ein Speicherplatz des Datenträgers angesteuert und die dort eingespeicherte Schlüsselzahl oder das Paßwort ausgelesen wird und daß anschließend der Benutzer beispielsweise über eine Anzeigevorrichtung des Endgeräts zur Eingabe der Schlüsselzahl oder des Paßworts aufgefordert wird, wobei der betreffende Speicherplatz für die Einspeicherung anderer Daten gesperrt ist.

Der Datenträger übernimmt damit praktisch die Aufgabe der Chipkarte. Solange nicht ein Datenträger benutzt wird, der an einer bestimmten Stelle die Schlüsselzahl oder das Paßwort enthält, kann das System nicht benutzt werden.

Eine Weiterbildung der Erfindung besteht darin, daß die Massenspeichereinrichtung einen kleinen, handlichen Datenträger, beispielsweise Mikro Floppy Disk, Mikrokassette, usw., aufweist.

Die Erfindung ist besonders vorteilhaft anwendbar, wenn der Datenträger klein und handlich, d. h. nur wenig größer als die Chipkarte ist.

Weitere Vorteile ergeben sich aus den Unteransprüchen.

Die Erfindung wird anhand eines Ausführungsbeispiels näher erläutert.

Bei dem Endgerät kann es sich beispielsweise um das Endgerät einer Datenverarbeitungseinrichtung, d. h. einen Personalcomputer handeln. In diesem Fall erfolgt die Zugriffssicherung bezüglich der Benutzung der Datenverarbeitungseinrichtung. Bei dem Endgerät kann es sich jedoch auch um das Endgerät einer Datenverarbeitungsanlage oder einer Fernmeldevermittlungsanlage handeln, wobei an derselben eine Vielzahl von Endgeräten angeschlossen ist und die Zugriffssicherung sich auf die Benutzung der Datenverarbeitungsanlage oder Fernmeldevermittlungsanlage bezieht. Es ist außerdem denkbar, daß das Endgerät als Datenverarbeitungseinrichtung ausgebildet ist und diese an einer Datenverarbeitungsanlage oder an einer Fernmeldevermittlungsanlage angeschlossen ist, wobei die Zugriffssicherung sich entweder nur auf die Datenverarbeitungseinrichtung oder nur auf die Benutzung der angeschlossenen Anlage oder auch auf beide Benutzungsfälle bezieht.

Ist ein Endgerät in der eingangs beschriebenen Art direkt mit einer fest zugeordneten Massenspeichereinrichtung wie beispielsweise Floppy Disk-Laufwerk, Mikro Floppy Disk-Laufwerk, Kassettenlaufwerk, Mikrokassetten-Laufwerk, usw., verbunden, so kann auf dem auswechselbaren Datenträger (Floppy Disk, Mikro Floppy Disk, Kassette, Mikrokassette, usw.,) ein bestimmter Speicherplatz freigehalten werden, der zum Eintragen der Schlüsselzahl oder des Paßwortes dient. Der Speicherplatz wird durch die Adresse aus einem Adressgenerator erzeugt, welcher Bestandteil der Steuereinrichtung des Endgeräts ist. Eine Inbetriebnahme des Endgeräts kann nur erfolgen, wenn der Datenträger in die Massenspeichereinrichtung eingelegt ist. Das Ansteuern des Speicherplatzes und das Auslesen der dort eingespeicherten Schlüsselzahl bzw. des Paßwortes kann nun entweder selbsttätig mit dem Einlegen des Datenträgers oder auch nach Betätigung einer bestimmten Taste der Eingabetastatur des Endgeräts erfolgen. Die ausgelesene Schlüsselzahl oder das Paßwort werden in der Steuereinrichtung des Endgeräts eingespeichert. Anschließend wird der Benutzer zur Eingabe der Schlüsselzahl oder des Paßworts aufgefordert. Dies kann beispielsweise über die Anzeigevorrichtung des Endgeräts erfolgen. Die über die Eingabetastatur eingegebene

Schlüsselzahl bzw. das über die Eingabetastur eingegebene Paßwort wird ebenfalls der Steuereinrichtung zugeführt und dort mit der aus dem Datenträger ausgelesenen Schlüsselzahl bzw. Paßwort verglichen. Stimmen beide überein, so wird das System zur Benutzung freigegeben.

Die Freigabe kann nun entweder gesperrt werden, sobald der Datenträger der Massenspeichereinrichtung wieder entnommen ist oder nach Betätigung einer bestimmten Taste. Es ist auch weiterhin möglich, eine zeitliche Überwachung der Benutzung des Endgeräts vorzunehmen, wobei nach Ablauf einer vorgegebenen Zeit die Benutzung des Endgeräts wieder gesperrt wird, wenn keine Benutzung mehr stattgefunden hat.

Selbstverständlich ist die Steuereinrichtung des Endgeräts so zu gestalten, daß beim Beschreiben des Datenträgers der für die Eintragung der Schlüsselzahl bzw. des Paßwortes benutzte Speicherplatz für diesen Zweck freigehalten wird. Das gleiche gilt für das Auslesen des Datenträgers, in diesem Fall muß der betreffende Speicherplatz übersprungen werden. Da sich die Schlüsselzahl oder das Paßwort im Datenformat nicht von den übrigen Daten auf dem Datenträger unterscheiden, dürfte es sehr schwer sein, die Schlüsselzahl oder das Paßwort auf dem Datenträger mit Hilfe eines anderen Endgeräts zu analysieren, zumal der Datenträger eine sehr große Datenmenge enthält und die Schlüsselzahl oder das Paßwort an beliebiger Stelle eingetragen sein können.

Zur Erhöhung der Sicherheit kann der Adressgenerator derart ausgebildet sein, daß die Adresse des Speicherplatzes mit jeder Benutzung des Endgerätes verändert wird. Dies hat zwar zur Folge, daß der gesamte Datenträger neu beschrieben werden muß, in vielen Fällen dürfte dies jedoch keine Schwierigkeiten bereiten, besonders wenn der gesamte Inhalt des Datenträgers in den Arbeitsspeicher des Endgeräts übertragen worden ist.

Eine weniger aufwendige Maßnahme besteht auch darin, daß dem Benutzer die Möglichkeit besteht, mit jeder Freigabe des Endgeräts die Schlüsselzahl oder das Paßwort zu ändern. Dies kann beispielsweise dadurch entstehen, daß nach Eingabe der Schlüsselzahl bzw. des Paßwortes und der Freigabe des Endgeräts zunächst die neue Schlüsselzahl oder ein neues Paßwort eingegeben wird, welches dann selbsttätig auf dem bestimmten Speicherplatz eingetragen wird.

Die Zugriffssicherung muß sich nun nicht auf sämtliche Funktionen des Endgeräts erstrecken, vielmehr ist auch eine Anwendung der Zugriffssicherung nur in bestimmten Fällen denkbar, beispielsweise wenn es sich bei dem Endgerät um ein solches handelt, welches an einer Fernmeldevermittlungsanlage angeschlossen ist. In diesem Fall kann die Zugriffssicherung beispielsweise auf die Herstellung von Fernverbindungen beschränkt sein, während die Benutzung des Endgeräts für den Aufbau einer Orts- Fernsprechverbindung, z. B in Notfällen freigegeben ist. Ein weiterer Anwendungsfall kann beispielsweise darin bestehen, die Zugriffssicherung auf die Änderung von Berechtigungen zu beschränken.

P 3954
25.3.85
Fs/Me.

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.